

PATENT COOPERATION TREATY

PCT

REC'D 22 MAR 2005

WIPO

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

10/530829

REPLACED BY

ART 34 AMDT

Applicant's or agent's file reference P17307-TPF	FOR FURTHER ACTION		See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/EP 03/10780	International filing date (day/month/year) 27.09.2003	Priority date (day/month/year) 11.10.2002	
International Patent Classification (IPC) or both national classification and IPC G06F1/00			
Applicant TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) et al.			

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.
 - This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 5 sheets.

3. This report contains indications relating to the following items:
 - I Basis of the opinion
 - II Priority
 - III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
 - IV Lack of unity of invention
 - V Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
 - VI Certain documents cited
 - VII Certain defects in the International application
 - VIII Certain observations on the International application

Date of submission of the demand 29.04.2004	Date of completion of this report 21.03.2005
Name and mailing address of the International preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized Officer Veillas, E Telephone No. +49 89 2399-6998



**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/EP 03/10780

I. Basis of the report

1. With regard to the elements of the international application (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17)*):

Description, Pages

1-26 as originally filed

Claims, Numbers

1-18 filed with telefax on 02.02.2005

Drawings, Sheets

1/3-3/3 as originally filed

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
- the language of publication of the international application (under Rule 48.3(b)).
- the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- contained in the international application in written form.
- filed together with the international application in computer readable form.
- furnished subsequently to this Authority in written form.
- furnished subsequently to this Authority in computer readable form.
- The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- the description, pages:
- the claims, Nos.:
- the drawings, sheets:

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/EP 03/10780

5. This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	1-18
	No: Claims	
Inventive step (IS)	Yes: Claims	1-18
	No: Claims	
Industrial applicability (IA)	Yes: Claims	1-18
	No: Claims	

2. Citations and explanations

see separate sheet

Re Item V

**Reasoned statement with regard to novelty, inventive step or industrial applicability:
citations and explanations supporting such statement**

- 1 Reference is made to the following document:

D1: N.Asokan et al, "Authenticating public terminals", Computer networks 31 (1999), Elsevier, pages 861-870

- 2 The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claim 1 does not involve an inventive step in the sense of Article 33(3) PCT.

- 2.1 The document D1 is regarded as being the closest prior art to the subject-matter of claim 1, and discloses (the references in parentheses applying to this document)a method (see the method described in section 3.3 for the rest of the mapping) being triggered by a request for linking (it is implicit that the issuance of the challenge/response pairs must be performed upon some request, either an invitation of the server or a request of the client. This request is de facto a request "for linking" the user home base with the untrusted terminal at a later stage. It is noted that the request of step 1 is posterior to the step of selecting the challenge/response pair and is thus not triggering this particular step) comprising the following steps:

- selecting a first linking information and a second linking information, the first linking information matching to the second linking information (the challenge sent on step 3 is a first linking information selected by the server and the challenge/response pairs sent to the user home base before his travel constitute the second linking information selected by the server. The first linking information matches the second linking information in that it is included in the second linking information).

-sending from the server the first linking information to the first device and the second linking information to the second device (see above, the first device is the untrusted public terminal and the second device is the trusted home base)

- presenting by the first device the first linking information and by the second device

the second linking information (the challenge sent on step 3 is presented on the untrusted terminal at step 4 and the challenge/response pair are presented at the home base since they are printed by the user)

- entering into the first device an indication of the matching of the first linking information and the second linking information (the user types in the response corresponding to the challenge in the untrusted terminal by looking it up in the list of challenge/response pairs)
- based on the entered indication of the matching, sending to the server a matching confirmation for confirming the matching to the server (step 6 : the untrusted terminal sends the response to the server as a confirmation of the matching)

- 2.2 The subject-matter of claim 1 differs thus from what is known from D1 in the step of associating a first characteristic of the first device and a second characteristic of the second device based upon the received matching information.
- 2.3 The differentiating feature of associating a characteristic of the first device and a characteristic of the second device based on the received matching information is considered to require technical considerations in that the association is made by the server (e.g. by correlating the characteristics in a table, see description page 7, lines 11-13). However this differentiating feature does not involve any technical effect and as a consequence does not solve any objective technical problem.
It is noted in particular that in a particular embodiment this association may only serve the purpose of carrying further processing of a statistical, commercial (charging) or legal nature (see page 3, lines 6-8 or page 8, lines 8-9). Therefore, this differentiating feature does not involve a technical contribution over the prior art document D1.
- 2.4 Consequently, the subject-matter of claim 1 does not involve an inventive step.
- 3 Independent claims 10 and 18 define a server comprising means to implement selected steps of method claim 1 and a computer program product comprising code adapted to execute the steps of method claim 1. Same objections thus apply to these claims.

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/EP 03/10780

- 4 Dependent claims 2-8, 10, 12-15 do not appear to contain any additional features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT with respect to inventive step, the reasons being as follows:
- 4.1 Claims 2-4, 6-8, 11-13 and 15-17 do not appear to contain features that confer a technical contribution over the prior art document D1 to the claimed subject-matter. The fact that the association is triggered by a request for authentication does not provide any technical effect to the association (it is also to be noted that a request for authentication is also present in D1, see step 1 of the message flow of paragraph 3.3). The mere fact that the first characteristic relates to an access legitimization does not have any technical effect. Further specifications of what constitute the linking information and the confirmation data do not confer a technical effect to the method as a whole since the only effect of the method as a whole remains that the characteristics of the first and second devices are associated.
- 4.2 Claims 3 and 14 specify that access to an institution is granted to/via the second device based on the association of the first characteristic relating to an access legitimization and the second characteristic comprising an identifier identifying the second device. The feature of granting access to an institution based on the confirmation of the matching of two linking informations is already implicitly known from D1 where access to a server from a public untrusted terminal is granted once authentication is performed (see paragraph 2). In the embodiment of section 3.3, the home base plays the role of a second trusted device participating in this authentication which permits a trusted path to be established between the user and the server through the untrusted public terminal. It appears that the feature of granting access to an institution based on an association between characteristics of devices, which association is carried out once authentication based on the matching of two linking informations has been confirmed does not contribute further to the technical character of the method because the intermediary step of associating the devices has apparently no technical contribution over the prior art document D1.

[Claims]

1. A method for linking of a first characteristic of a first device (PP1,PP2) and a second characteristic of a second device (NP1,NP2) by a server (S1,AS2), the method being triggered by a request (50) for linking and comprising the following steps of:
 - selecting (75) a first linking information and a second linking information, the first linking information matching to the second linking information,
 - sending (100,150) from the server (S1,AS2) the first linking information to the first device (PP1,PP2) and the second linking information to the second device (NP1,NP2),
 - presenting (200,250) by the first device (PP1,PP2) the first linking information and by the second device (NP1,NP2) the second linking information,
 - entering (300) into the first device (PP1,PP2) an indication of the matching of the first linking information and the second linking information,
 - based on the entered indication of the matching, sending (400) to the server (S1,AS2) a matching confirmation for confirming the matching to the server (S1,AS2),
 - associating (450) the first characteristic and the second characteristic based on the received matching confirmation.
- 25 2. The method according to claim 1, wherein the method is used for authentication, the request (50) for linking is a request for authentication and the first device (PP1,PP2) is a trusted device, further comprising the step of stating the association (450) by an authentication assertion.
- 30 3. The method according to claim 2, wherein the authentication assertion is sent for granting access.

4. The method according to any of the preceding claims, wherein the first device (PP1,PP2) is a trusted device and the first characteristic relates to an access legitimization legitimating the trusted device for accessing a first institution.
5. The method according to claim 4, wherein the second characteristic comprises an identifier identifying the second device (NP1,NP2) and access to a second institution is granted to or via the second device (NP1,NP2) based on the associating (450) of the first characteristic relating to the access legitimization and the second characteristic comprising the identifier, the second institution being identical to or different from the first institution.
- 10 6. The method according to any of the preceding claims, wherein the first linking information and the second linking information comprise one or more randomly generated symbols.
- 15 7. The method according to any of the preceding claims, wherein the first linking information is identical to the second linking information.
- 20 8. The method according to any of the preceding claims, wherein the associating (450) is based on a verification for correctness of confirmation data entered into the first device (PP1,PP2).
- 25 9. The method according to claim 8, wherein the entered confirmation data comprises at least one of
 - (a) a Personal Identification Number,
 - (b) a password,
- 30 (c) an indication for additional information being presented in parallel to the first linking information or second linking information, the additional information being

distinguishable from the first linking information and the second linking information, and

- (d) data being computed on the base of the first linking information and/or the second linking information.

5

10. A server (S1,AS2) usable for linking of a first characteristic of a first device (PP1,PP2) and a second characteristic of a second device (NP1,NP2), the server (S1,AS2) comprising a receiving unit for receiving messages, a transmitting unit for sending messages, and a processing unit for processing messages and information, wherein

10. the receiving unit is adapted to receive a request (50) for linking, the processing unit is adapted to be triggered by the received request (50) for linking and to select a first linking information and a second linking information, the first linking information matching to the second linking information, the transmission unit is adapted to send the first

15. linking information to the first device (PP1,PP2) and the second linking information to the second device (NP1,NP2), the receiving unit is adapted to receive a matching confirmation from the first device (PP1,PP2), the matching confirmation confirming to the processing unit the matching of the first linking information presented by the first device (PP1,PP2) and the second linking information presented by the second device (NP1,NP2), and the processing unit is adapted to execute an associating (450) of the first characteristic and the second characteristic based on the received matching confirmation.

20. 25. The server (S1,AS2) according to claim 10, wherein the server (S1,AS2) is used for authentication, the request (50) for linking is a request for authentication and the first device (PP1,PP2) is a trusted device, the processing unit being further adapted to state the association (450) by an authentication assertion.

12. The server (S1,AS2) according to claim 11, wherein the transmission unit is adapted to send the authentication assertion for granting access.
- 5 13. The server (S1,AS2) according to any of the claims 10 to 12, wherein the first device (PP1,PP2) is a trusted device and the first characteristic relates to an access legitimization legitimating the trusted device for accessing a first institution.
- 10 14. The server (S1,AS2) according to claim 13, wherein the second characteristic comprises an identifier identifying the second device and, based on the associating (450) of the first characteristic relating to the access legitimization and the second characteristic comprising the identifier, the processing unit is adapted to generate an access assertion for granting to or via the second device (NP1,NP2) access to a second institution being identical or different from the first institution, and the transmission unit is adapted to send the access assertion to the second device (NP1,NP2) or the second institution or to an entity supporting the second device (NP1,NP2) or the second institution for granting access.
- 15 15. The server (S1,AS2) according to any of the claims 10 to 14, wherein the processing unit is adapted to select the first linking information and the second linking information to comprise one or more randomly generated symbols.
- 20 16. The server (S1,AS2) according to any of the claims 10 to 15, wherein the processing unit is adapted to select the first linking information being identical to the second linking information.
- 25 17. The server (S1,AS2) according to any of the claims 10 to 16, wherein the processing unit is adapted to execute the associating (450) of the

first characteristic and the second characteristic based on a verification for correctness of confirmation data entered into the first device (PP1,PP2).

- 5 18. A computer program usable for linking of a first characteristic of a first device (PP1,PP2) and a second characteristic of a second device (NP1,NP2), the computer program being loadable into a processing unit of a server (S1,AS2), wherein the computer program comprises code adapted to be triggered by a request (50) for linking, to select a
10 first linking information and a second linking information, the first linking information matching to the second linking information, to initialize a sending of the first linking information to the first device (PP1,PP2) and a sending of the second linking information to the second device (NP1,NP2), and to execute an associating (450) of the
15 first characteristic and the second characteristic based on a matching confirmation received from the first device (PP1,PP2), the matching confirmation confirming to the computer program the matching of the first linking information presented by the first device (PP1,PP2) and the second linking information presented by the second device (NP1,NP2).
20

P17307-TPF

ART 3A AMDT

[Claims]

1. A method for linking of a first characteristic of a first device (PP1,PP2) and a second characteristic of a second device (NP1,NP2) by a server (S1,AS2), the method being triggered by a request (50) for linking and comprising the following steps of:
 - selecting (75) a first linking information and a second linking information, the first linking information matching to the second linking information,
 - sending (100,150) from the server (S1,AS2) the first linking information to the first device (PP1,PP2) and the second linking information to the second device (NP1,NP2),
 - presenting (200,250) by the first device (PP1,PP2) the first linking information and by the second device (NP1,NP2) the second linking information,
 - entering (300) into the first device (PP1,PP2) an indication of the matching of the first linking information and the second linking information,
 - based on the entered indication of the matching, sending (400) to the server (S1,AS2) a matching confirmation for confirming the matching to the server (S1,AS2),
 - associating (450) the first characteristic and the second characteristic based on the received matching confirmation.
2. The method according to claim 1, wherein the method is used for authentication, the request (50) for linking is a request for authentication and the first device (PP1,PP2) is a trusted device, further comprising the step of stating the association (450) by an authentication assertion.
3. The method according to claim 2, wherein the authentication assertion is sent for granting access.

P17307-TPF

28

- ART 21 AMDT
4. The method according to any of the preceding claims, wherein the first device (PP1,PP2) is a trusted device and the first characteristic relates to an access legitimization legitimating the trusted device for accessing a first institution.
 5. The method according to claim 4, wherein the second characteristic comprises an identifier identifying the second device (NP1,NP2) and access to a second institution is granted to or via the second device (NP1,NP2) based on the associating (450) of the first characteristic relating to the access legitimization and the second characteristic comprising the identifier, the second institution being identical to or different from the first institution.
 - 10 6. The method according to any of the preceding claims, wherein the first linking information and the second linking information comprise one or more randomly generated symbols.
 - 15 7. The method according to any of the preceding claims, wherein the first linking information is identical to the second linking information.
 - 20 8. The method according to any of the preceding claims, wherein the associating (450) is based on a verification for correctness of confirmation data entered into the first device (PP1,PP2).
 - 25 9. The method according to claim 8, wherein the entered confirmation data comprises at least one of
 - (a) a Personal Identification Number,
 - (b) a password;
 - 30 (c) an indication for additional information being presented in parallel to the first linking information or second linking information, the additional information being

P17307-TPF

ART 2A AMDT

distinguishable from the first linking information and the second linking information, and

(d) data being computed on the base of the first linking information and/or the second linking information.

5

10. A server (S1,AS2) usable for linking of a first characteristic of a first device (PP1,PP2) and a second characteristic of a second device (NP1,NP2), the server (S1,AS2) comprising a receiving unit for receiving messages, a transmitting unit for sending messages, and a processing unit for processing messages and information, wherein the receiving unit is adapted to receive a request (50) for linking, the processing unit is adapted to be triggered by the received request (50) for linking and to select a first linking information and a second linking information, the first linking information matching to the second linking information, the transmission unit is adapted to send the first linking information to the first device (PP1,PP2) and the second linking information to the second device (NP1,NP2), the receiving unit is adapted to receive a matching confirmation from the first device (PP1,PP2), the matching confirmation confirming to the processing unit the matching of the first linking information presented by the first device (PP1,PP2) and the second linking information presented by the second device (NP1,NP2), and the processing unit is adapted to execute an associating (450) of the first characteristic and the second characteristic based on the received matching confirmation.
- 15
- 20
- 25
30. 11. The server (S1,AS2) according to claim 10, wherein the server (S1,AS2) is used for authentication, the request (50) for linking is a request for authentication and the first device (PP1,PP2) is a trusted device, the processing unit being further adapted to state the association (450) by an authentication assertion.

P17307-TPF

30

- ART 31 AMDT
12. The server (S1,AS2) according to claim 11, wherein the transmission unit is adapted to send the authentication assertion for granting access.
- 5 13. The server (S1,AS2) according to any of the claims 10 to 12, wherein the first device (PP1,PP2) is a trusted device and the first characteristic relates to an access legitimization legitimating the trusted device for accessing a first institution.
- 10 14. The server (S1,AS2) according to claim 13, wherein the second characteristic comprises an identifier identifying the second device and, based on the associating (450) of the first characteristic relating to the access legitimization and the second characteristic comprising the identifier, the processing unit is adapted to generate an access assertion for granting to or via the second device (NP1,NP2) access to a second institution being identical or different from the first institution, and the transmission unit is adapted to send the access assertion to the second device (NP1,NP2) or the second institution or to an entity supporting the second device (NP1,NP2) or the second institution for granting access.
- 15 20
- 25
15. The server (S1,AS2) according to any of the claims 10 to 14, wherein the processing unit is adapted to select the first linking information and the second linking information to comprise one or more randomly generated symbols.
- 30 16. The server (S1,AS2) according to any of the claims 10 to 15, wherein the processing unit is adapted to select the first linking information being identical to the second linking information.
17. The server (S1,AS2) according to any of the claims 10 to 16, wherein the processing unit is adapted to execute the associating (450) of the

P17307-TPF

31

first characteristic and the second characteristic based on a verification for correctness of confirmation data entered into the first device (PP1,PP2).

- 5 18. A computer program usable for linking of a first characteristic of a first device (PP1,PP2) and a second characteristic of a second device (NP1,NP2), the computer program being loadable into a processing unit of a server (S1,AS2), wherein the computer program comprises code adapted to be triggered by a request (50) for linking, to select a
10 first linking information and a second linking information, the first linking information matching to the second linking information, to initialize a sending of the first linking information to the first device (PP1,PP2) and a sending of the second linking information to the second device (NP1,NP2), and to execute an associating (450) of the first characteristic and the second characteristic based on a matching confirmation received from the first device (PP1,PP2), the matching confirmation confirming to the computer program the matching of the first linking information presented by the first device (PP1,PP2) and the second linking information presented by the second device (NP1,NP2).
15
20